

**Notice of Allowability**

Application No.

09/869,435

Applicant(s)

GOUBIN, LOUIS

Examiner

LEYNNA T. HA

Art Unit

2135

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 3/7/2005.
2. ☒ The allowed claim(s) is/are 1,5-8,10 and 11.
3. ☐ The drawings filed on \_\_\_\_\_ are accepted by the Examiner.
4. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
  - a) ☒ All    b) ☐ Some\*    c) ☐ None    of the:
    1. ☒ Certified copies of the priority documents have been received.
    2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  6. ☒ CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
    - (b) ☒ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date 5/25/2005.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).**
7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date 5/25/2005.
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_.

**DETAILED ACTION**

1. Claims 1-11 are pending.

Claims 2-4 and 9 are cancelled by Applicant.

2. Claims 1, 8, and 10 have further been amended through Examiner's Amendment. Please replace claims 1, 8, and 10.

**EXAMINER'S AMENDMENT**

3. **An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.**

Authorization for this examiner's amendment was given in a telephone interview with Mr. Jason Vick on May 26, 2005.

**The application has been amended as follows:**

**Replace claim 1:** A method adapted to protect a smart card implementing a cryptographic process involving calculation of a modular exponentiation of a quantity (x), said modular exponentiation using a secret exponent (d), comprising breaking down said secret exponent (d) into

unpredictable values ( $d_1, d_2, \dots, d_k$ ), wherein  $k$  is greater than 2, and at least one of said ( $k-1$ ) values has a length at least equal to 64 bits, the sum of which is equal to said secret exponent ( $d$ ) including:

deriving ( $k-1$ ) unpredictable values ( $d_1, d_2, \dots, d_{k-1}$ ), using a random generator;

obtaining a final unpredictable value ( $d_k$ ) from the difference between the secret exponent ( $d$ ) and the ( $k-1$ ) unpredictable values ( $d_1, d_2, \dots, d_{k-1}$ ),

creating  $k$  intermediate results by performing modular exponentiation on the quantity ( $x$ ) using the  $k$  unpredictable values ( $d_1, d_2, \dots, d_{k-1}, d_k$ ); and

calculating a final results based on the  $k$  intermediate results, equal to the modular exponentiation of the quantity ( $x$ ) using the secret exponent ( $d$ ).

**Replace claim 5:** Utilizing the method according to claim 1 in the smart card comprising information processing means.

**Replace claim 8:** A method adapted to protect a smart card implementing a cryptographic process involving calculation of a modular exponentiation of a quantity ( $x$ ), said modular exponentiation using a secret exponent ( $d$ ), comprising:

breaking down said secret exponent ( $d$ ) into a plurality of  $k$  unpredictable values ( $d_1, d_2, \dots, d_k$ ), the sum of which is equal to said secret exponent;

obtaining said unpredictable value ( $d_1, d_2, \dots, d_k$ ) by deriving  $(k-1)$  values by means of a random generator,

wherein  $k$  is greater than 2, and at least one of said  $(k-1)$  values has a length at least equal to 64 bits, by raising the quantity ( $x$ ) by an exponent comprising a final value and obtaining a set of results for each of said  $k$  values and calculating a product of the set of results and taking the difference between the secret exponent and the  $(k-1)$  values to derive the final value.

**Replace claim 10:** A smart card adapted to protect an electronic system comprising:

means for implementing a cryptographic process involving calculation of a modular exponentiation of a quantity ( $x$ ), said modular exponentiation using a secret exponent ( $d$ ), comprising:

means for breaking down said secret exponent ( $d$ ) into a plurality of  $k$  unpredictable values ( $d_1, d_2, \dots, d_k$ ), the sum of which is equal to said secret exponent, means for obtaining said unpredictable value ( $d_1, d_2, \dots, d_k$ ) by a random generator for deriving  $(k-1)$  values, wherein  $k$  is greater than 2, and at least one of said  $(k-1)$  values has a length at least equal to 64 bits, and means for taking the difference between the secret exponent and the  $(k-1)$  values to derive the final value.

***Allowable Subject Matter***

4. Claims 1, 5-8, and 10-11 are allowed over art.

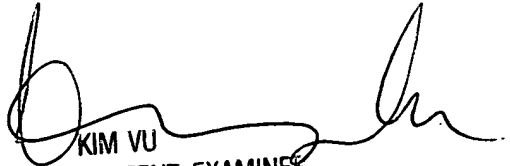
***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100